Azure Stack Operator Documentation

Overview

What is Azure Stack?
Comparing the Azure ecosystem

Release notes

Recent updates
1903 update
1902 update
1901 update
1811 update

Quickstarts

Use the administration portal

Tutorials

Offer Virtual Machines
Offer SQL databases
Offer highly available SQL databases
Offer highly available MySQL databases
Offer Web Apps

Concepts

Capacity Planning

Compute capacity planning
Storage capacity planning
Azure Stack Capacity Planner

Datacenter integration

General Azure Stack integration considerations
Azure Stack deployment connection models
Connected deployment considerations
Disconnected deployment considerations
Datacenter network integration
Network integration
Border connectivity
DNS integration
Firewall integration
Publish endpoints
Extension host
Identity integration
Choose an identity provider
Create registration role
Validate Azure identity
Validate ADFS integration
Validate graph integration
Azure Stack deployment PKI requirements
Generate PKI certificates
Prepare Azure Stack PKI certificates
Validate PKI certificates
Remediate PKI certificates
Deployment resources
About deployment networking
Validate Azure registration
Start-AzsReadiness cmdlet reference
View the readiness report
External monitoring
External auditing
Syslog forwarding
Device auditing
How-to guides
Manage Azure Stack
Administration basics
Configure telemetry collection
Register Azure Stack
Region management
Connect to Azure using ExpressRoute
Enable CLI for users
Set up management environment
  Install Azure Stack PowerShell
  Download tools
  Connect with PowerShell
Access privileged endpoint
Manage updates
  Manage updates overview
  Apply updates
  Monitor update status
Monitor health and alerts
Manage network resources
Change user subscription owner
Start and stop Azure Stack
Manage capacity
  Manage storage resources
  Manage storage capacity
  Manage storage infrastructure
  Manage physical memory capacity
  Add scale unit nodes
  Add public IP addresses
Replace hardware
  Node actions
  Replace node
  Replace disk
  Replace component
Security, compliance & identity
  Security overview
Identity
  Identity overview
  Identity architecture
Manage RBAC
Add users for Azure AD
Add users for AD FS
Create service principals
Enable multi-tenancy
Data at rest encryption
Rotate secrets
Update antivirus
Log collection and data handling
Populate the marketplace
Marketplace overview
Download marketplace items
Azure Marketplace items for Azure Stack
Create and publish a marketplace item
Supported guest operating systems for Azure Stack
Add a custom virtual machine image
Offer a virtual machine scale set
Windows Server in Marketplace FAQ
Offer Linux virtual machines
Add a Red Hat virtual machine
Offer a Kubernetes Cluster
Create a site-to-site VPN connection
Offer services
Offer SQL as PaaS
Deploy the SQL Server resource provider
Add SQL hosting servers
Create SQL databases
Update the SQL Server resource provider
Maintain the SQL Server resource provider
Remove the SQL Server resource provider
SQL resource provider release notes
  SQL resource provider 1.1.30.0 release notes
SQL resource provider 1.1.33.0 release notes

Offer MySQL as PaaS
Deploy the MySQL Server resource provider
Add MySQL hosting servers
Create MySQL Databases
Update the MySQL Server resource provider
Maintain MySQL Server resource provider
Remove the MySQL Server resource provider
MySQL resource provider release notes
  MySQL resource provider 1.1.30.0 release notes
  MySQL resource provider 1.1.33.0 release notes

Offer App Service as PaaS
App Service capacity planning
Before you get started
Deploy App Service
Deploy App Service for high availability
Deploy App Service offline
Update App Service
Update App Service Offline
Add App Service infrastructure roles
Configure deployment sources
Back up App Service
Recover App Service
App Service on Azure Stack release notes
  App Service on Azure Stack update 1 release notes
  App Service on Azure Stack update 2 release notes
  App Service on Azure Stack update 3 release notes
  App Service on Azure Stack update 4 release notes
  App Service on Azure Stack update 5 release notes

Create plans, offers, and quotas
  Plan, offer, quota, and subscription overview
  Create a plan
Create an add-on plan
Create an offer
Subscribe to an offer
Delegate offers in Azure Stack
Quota types
Usage and billing
Manage usage and billing as a CSP
  Add tenants for usage and billing
  Manage tenant registration
Usage and billing reference
  Usage data reporting
  Usage reporting infrastructure for Cloud Service Providers
  Provider usage API
  Tenant usage API
  Usage FAQ
Back up Azure Stack
  Enable Backup for Azure Stack from the administration console
  Enable Backup for Azure Stack with PowerShell
Back up Azure Stack
Back up files and applications on Azure Stack
Replicate Azure Stack VMs to Azure
Recover from catastrophic data loss
Backup best practices
Backup reference
Troubleshoot
  Known issues
  Diagnostics in Azure Stack
  Validation for Azure Stack
Reference
  Azure Stack PowerShell
Related
  Azure Stack User Documentation
2 minutes to read
2 minutes to read
2 minutes to read
2 minutes to read
2 minutes to read
2 minutes to read
2 minutes to read
2 minutes to read
2 minutes to read
You can use Azure Backup to protect (or back up) files and applications on Azure Stack. To back up files and applications, install Microsoft Azure Backup Server as a virtual machine running on Azure Stack. You can protect the files on any Azure Stack server in the same virtual network. Once you have installed Azure Backup Server, add Azure disks to increase the local storage available for short-term backup data. Azure Backup Server uses Azure storage for long-term retention.

**NOTE**

Though Azure Backup Server and System Center Data Protection Manager (DPM) are similar, DPM is not supported for use with Azure Stack.

This article does not cover installing Azure Backup Server in the Azure Stack environment. To install Azure Backup Server on Azure Stack, see the article, [Installing Azure Backup Server](#).

### Back up Files and Folders in Azure Stack VMs to Azure

To configure Azure Backup Server to protect Files in Azure Stack virtual machines, open the Azure Backup Server console. You’ll use the console to configure protection groups and to protect the data on your virtual machines.

1. In the Azure Backup Server console, click **Protection** and in the toolbar, click **New** to open the **Create New Protection Group** wizard.

   ![Create New Protection Group wizard](#)

   It may take a few seconds for the wizard to open. Once the wizard opens, click **Next** to advance to the **Select Protection Group Type** screen.
2. On the Select Protection Group Type screen, choose Servers and click Next.

The Select Group Members screen opens.
3. In the **Select Group Members** screen, click + to expand the list of subitems. For all items that you want to protect, select the check box. Once all items have been selected, click **Next**.

Microsoft recommends putting all data that will share a protection policy, into one protection group. For complete information about planning and deploying protection groups, see the System Center DPM article, [Deploy Protection Groups](#).

4. In the **Select Data Protection Method** screen, type a name for the protection group. Select the checkbox for **I want short-term protection using:** and **I want online protection**. Click **Next**.
To select **I want online protection**, you must first select **I want short-term protection using**: Disk. Azure Backup Server does not protect to tape, so disk is the only choice for short-term protection.

5. In the **Specify Short-Term Goals** screen, choose how long to retain the recovery points saved to disk, and when to save incremental backups. Click **Next**.

![Select Data Protection Method](image)

**IMPORTANT**

You should **not** retain operational recovery (backup) data on Azure Backup Server-attached disks for more than five days.

![Specify Short-Term Goals](image)

Instead of selecting an interval for incremental backups, to run an express full backup just before each scheduled recovery point, click **Just before a recovery point**. If you’re protecting application workloads, Azure Backup Server creates recovery points per the Synchronization frequency schedule (provided the application supports incremental backups). If the application doesn’t support incremental backups, Azure Backup Server runs an express full backup.

For **File recovery points**, specify when to create recovery points. Click **Modify** to set the times and days of the week when recovery points are created.

6. In the **Review disk allocation** screen, review the storage pool disk space allocated for the protection group.

**Total Data size** is the size of the data you want to back up and **Disk space to be provisioned** on Azure Backup Server is the recommended space for the protection group. Azure Backup Server chooses the ideal backup volume, based on the settings. However, you can edit the backup volume choices in the Disk allocation details. For the workloads, select the preferred storage in the dropdown menu. Your edits change the values for Total Storage and Free Storage in the Available Disk Storage pane. Underprovisioned space is the amount of storage Azure Backup Server suggests you add to the volume, to continue with backups smoothly in the future.

7. In **Choose replica creation method**, select how you want to handle the initial full data replication. If you decide to replicate over the network, Azure recommends you choose an off-peak time. For large amounts of
data or less than optimal network conditions, consider replicating the data using removable media.

8. In **Choose consistency check options**, select how you want to automate consistency checks. Enable consistency checks to run only when data replication becomes inconsistent, or according to a schedule. If you don't want to configure automatic consistency checking, run a manual check at any time by:
   - In the **Protection** area of the Azure Backup Server console, right-click the protection group and select **Perform Consistency Check**.

9. If you choose to back up to Azure, on the **Specify online protection data** page make sure the workloads you want to back up to Azure are selected.

10. In **Specify online backup schedule**, specify when incremental backups to Azure should occur.

    You can schedule backups to run every day/week/month/year and the time/date at which they should run. Backups can occur up to twice a day. Each time a backup job runs, a data recovery point is created in Azure from the copy of the backed-up data stored on the Azure Backup Server disk.

11. In **Specify online retention policy**, specify how the recovery points created from the daily/weekly/monthly/yearly backups are retained in Azure.

12. In **Choose online replication**, specify how the initial full replication of data occurs.

13. On **Summary**, review your settings. When you click **Create Group**, the initial data replication occurs. When the data replication finishes, on the **Status** page, the protection group status shows as **OK**. The initial backup job takes place in line with the protection group settings.

---

**Recover file data**

Use Azure Backup Server console to recover data to your virtual machine.

1. In the Azure Backup Server console, on the navigation bar, click **Recovery** and browse for the data you want to recover. In the results pane, select the data.

2. On the calendar in the recovery points section, dates in bold indicate recovery points are available. Select the date to recover.

3. In the **Recoverable item** pane, select the item you want to recover.

4. In the **Actions** pane, click **Recover** to open the Recovery Wizard.

5. You can recover data as follows:
   - **Recover to the original location** - If the client computer is connected over VPN, this option doesn’t work. Instead use an alternate location, and then copy data from that location.
   - **Recover to an alternate location**

6. Specify the recovery options:
   - **For Existing version recovery behavior**, select **Create copy**, **Skip**, or **Overwrite**. Overwrite is available only when recovering to the original location.
   - **For Restore security**, choose **Apply settings of the destination computer** or **Apply the security settings of the recovery point version**.
   - **For Network bandwidth usage throttling**, click **Modify** to enable network bandwidth usage throttling.
   - **Notification** Click **Send an e-mail when the recovery completes**, and specify the recipients who will receive the notification. Separate the e-mail addresses with commas.

7. Review your recovery settings, and click **Recover**.
NOTE
While the recovery job is in progress, all synchronization jobs for the selected recovery items are canceled.

If you’re using Modern Backup Storage (MBS), File Server end-user recovery (EUR) isn’t supported. File Server EUR has a dependency on Volume Shadow Copy Service (VSS), which Modern Backup Storage doesn’t use. If EUR is enabled, use the following steps to recover data:

1. Navigate to the protected files, and right-click the file name and select Properties.
2. On the Properties menu, click Previous Versions and choose the version you want to recover.

View Azure Backup Server with a vault

To view Azure Backup Server entities in Azure Portal, you can follow the following steps:

1. Open Recovery Services vault.
2. Click Backup Infrastructure.

See also

For information on using Azure Backup Server to protect other workloads, see one of the following articles:

- Back up SharePoint farm
- Back up SQL server
This article shows you how to set up disaster recovery Azure Stack VMs to Azure, using the Azure Site Recovery service.

Site Recovery contributes to your business continuity and disaster recovery (BCDR) strategy. The service ensures that your VM workloads remain available when expected and unexpected outages occur.

- Site Recovery orchestrates and manages replication of VMs to Azure storage.
- When an outage occurs in your primary site, you use Site Recovery to fail over to Azure.
- On failover, Azure VMs are created from the stored VM data, and users can continue accessing workloads running on those Azure VMs.
- When everything's up and running again, you can fail back Azure VMs to your primary site, and start replicating to Azure storage again.

In this article, you learn how to:

- **Step 1: Prepare Azure stack VMs for replication.** Check that VMs comply with Site Recovery requirements, and prepare for installation of the Site Recovery Mobility service. This service is installed on each VM you want to replicate.
- **Step 2: Set up a Recovery Services vault.** Set up a vault for Site Recovery, and specify what you want to replicate. Site Recovery components and actions are configured and managed in the vault.
- **Step 3: Set up the source replication environment.** Set up a Site Recovery configuration server. The configuration server is a single Azure Stack VM that runs all the components needed by Site Recovery. After you've set up the configuration server, you register it in the vault.
- **Step 4: Set up the target replication environment.** Select your Azure account, and the Azure storage account and network that you want to use. During replication, VM data is copied to Azure storage. After failover, Azure VMs are joined to the specified network.
- **Step 5: Enable replication.** Configure replication settings, and enable replication for VMs. The Mobility service will be installed on a VM when replication is enabled. Site Recovery performs an initial replication of the VM, and then ongoing replication begins.
- **Step 6: Run a disaster recovery drill.** After replication is up and running, you verify that failover will work as expected by running a drill. To initiate the drill, you run a test failover in Site Recovery. The test failover doesn’t impact your production environment.

With these steps complete, you can then run a full failover to Azure as and when you need to.

**Architecture**
**Configuration server**

- Runs on a single Azure Stack VM.
- In each subscription you set up a configuration server VM. This VM runs the following Site Recovery components:
  - Configuration server: Coordinates communications between on-premises and Azure, and manages data replication.
  - Process server: Acts as a replication gateway. It receives replication data, optimizes with caching, compression, and encryption; and sends it to Azure storage.
  - If VMs you want to replicate exceed the limits stated below, you can set up a separate standalone process server.

**Mobility service**

- Installed on each VM you want to replicate.
- In the steps in this article, we prepare an account so that the Mobility service is installed automatically on a VM when replication is enabled. If you don't want to install the service automatically, there are a number of other methods you can use. Learn more.

**Azure**

- In Azure you need a Recovery Services vault, a storage account, and a virtual network.
- Replicated data is stored in the storage account. Azure VMs are added to the Azure network when failover occurs.

Replication works as follows:

1. In the vault, you specify the replication source and target, set up the configuration server, create a replication policy, and enable replication.
2. The Mobility service is installed on the machine (if you've used push installation), and machines begin replication in accordance with the replication policy.
3. An initial copy of the server data is replicated to Azure storage.
4. After initial replication finishes, replication of delta changes to Azure begins. Tracked changes for a machine are held in a .hrl file.
5. The configuration server orchestrates replication management with Azure (port HTTPS 443 outbound).
6. The process server receives data from source machines, optimizes and encrypts it, and sends it to Azure storage (port 443 outbound).
7. Replicated machines communicate with the configuration server (port HTTPS 443 inbound, for replication management. Machines send replication data to the process server (port HTTPS 9443 inbound - can be modified).
8. Traffic is replicated to Azure storage public endpoints, over the internet. Alternately, you can use Azure ExpressRoute public peering. Replicating traffic over a site-to-site VPN from an on-premises site to Azure isn’t supported.

**Prerequisites**

Here’s what you need to set up this scenario.

<table>
<thead>
<tr>
<th>REQUIREMENT</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure subscription account</td>
<td>If you don’t have an Azure subscription, create a <a href="#">free account</a>.</td>
</tr>
<tr>
<td>Azure account permissions</td>
<td>The Azure account you use needs permissions to:</td>
</tr>
<tr>
<td></td>
<td>· Create a Recovery Service vault</td>
</tr>
<tr>
<td></td>
<td>· Create a virtual machine in the resource group and virtual network you use for the scenario</td>
</tr>
<tr>
<td></td>
<td>· Write to the storage account you specify</td>
</tr>
<tr>
<td></td>
<td>Note that:</td>
</tr>
<tr>
<td></td>
<td>· If you create an account, you’re the administrator of your subscription and can perform all actions.</td>
</tr>
<tr>
<td></td>
<td>· If you use an existing subscription and you’re not the administrator, you need to work with the admin to assign you Owner or Contributor permissions.</td>
</tr>
<tr>
<td></td>
<td>· If you need more granular permissions, review <a href="#">this article</a>.</td>
</tr>
<tr>
<td>Azure Stack VM</td>
<td>You need an Azure Stack VM in the tenant subscription, that will be deployed as the Site Recovery configuration server.</td>
</tr>
</tbody>
</table>

**Prerequisites for the configuration server**

**Configuration/Process server requirements for physical server replication**

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>HARDWARE SETTINGS</td>
<td></td>
</tr>
<tr>
<td>CPU cores</td>
<td>8</td>
</tr>
<tr>
<td>RAM</td>
<td>16 GB</td>
</tr>
<tr>
<td>COMPONENT</td>
<td>REQUIREMENT</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Number of disks</td>
<td>3, including the OS disk, process server cache disk, and retention drive for failback</td>
</tr>
<tr>
<td>Free disk space (process server cache)</td>
<td>600 GB</td>
</tr>
<tr>
<td>Free disk space (retention disk)</td>
<td>600 GB</td>
</tr>
</tbody>
</table>

**SOFTWARE SETTINGS**

- Operating system locale: English (en-us)
- Windows Server roles: Don’t enable these roles: - Active Directory Domain Services - Internet Information Services - Hyper-V
- Group policies: Don’t enable these group policies: - Prevent access to the command prompt. - Prevent access to registry editing tools. - Trust logic for file attachments. - Turn on Script Execution. Learn more
- IIS: - No preexisting default website - No preexisting website/application listening on port 443 - Enable anonymous authentication - Enable FastCGI setting.
- IP address type: Static

**ACCESS SETTINGS**

- MYSQL: MySQL should be installed on the configuration server. You can install manually, or Site Recovery can install it during deployment. For Site Recovery to install, check that the machine can reach http://cdn.mysql.com/archives/mysql-5.5/mysql-5.5.37-win32.msi.
### URLs

The configuration server needs access to these URLs (directly or via proxy):

**Azure AD:**
- login.microsoftonline.com
- login.microsoftonline.us
- *.accesscontrol.windows.net

**Replication data transfer:**
- *.backup.windowsazure.com
- *.backup.windowsazure.us

**Replication management:**
- *.hypervrecoverymanager.windowsazure.com
- *.hypervrecoverymanager.windowsazure.us
- https://management.azure.com
- *.services.visualstudio.com

**Storage access:**
- *.blob.core.windows.net
- *.blob.core.usgovcloudapi.net

**Time synchronization:**
- time.nist.gov
- time.windows.com

**Telemetry (optional):**
- dc.services.visualstudio.com

---

### Firewall

IP address-based firewall rules should allow communication to Azure URLs. To simplify and limit the IP ranges, we recommend using URL filtering.

**For commercial IPs:**
- Allow the [Azure Datacenter IP Ranges](#), and the HTTPS (443) port.
- Allow IP address ranges for the West US (used for Access Control and Identity Management).
- Allow IP address ranges for the Azure region of your subscription, to support the URLs needed for Azure Active Directory, backup, replication, and storage.

**For government IPs:**
- Allow the Azure Government Datacenter IP Ranges, and the HTTPS (443) port.
- Allow IP address ranges for all US Gov Regions (Virginia, Texas, Arizona, and Iowa), to support the URLs needed for Azure Active Directory, backup, replication, and storage.

---

### Ports

- Allow 443 (Control channel orchestration)
- Allow 9443 (Data transport)

---

**Configuration/Process server sizing requirements**
### CPU
- 8 vCPUs
  - 2 sockets * 4 cores @ 2.5 GHz
  - 16GB
  - 300 GB
  - 500 GB or less
  - < 100 machines

- 12 vCPUs
  - 2 sockets * 6 cores @ 2.5 GHz
  - 18GB
  - 600 GB
  - 500 GB-1 TB
  - 100 to 150 machines

- 16 vCPUs
  - 2 sockets * 8 cores @ 2.5 GHz
  - 32 GB
  - 1 TB
  - 1-2 TB
  - 150 -200 machines

---

### Step 1: Prepare Azure Stack VMs

#### Verify the operating system

Make sure that the VMs are running one of the operating systems summarized in the table.

<table>
<thead>
<tr>
<th>OPERATING SYSTEM</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS</td>
<td>5.2 to 5.11, 6.1 to 6.9, 7.0 to 7.3</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>14.04 LTS server, 16.04 LTS server. Review supported kernels</td>
</tr>
</tbody>
</table>

#### Prepare for Mobility service installation

Every VM you want to replicate must have the Mobility service installed. In order for the process server to install the service automatically on the VM when replication is enabled, verify the VM settings.

**Windows machines**

- You need network connectivity between the VM on which you want to enable replication, and the machine running the process server (by default this is the configuration server VM).
- You need an account with admin rights (domain or local) on the machine for which you enable replication.
  - You specify this account when you set up Site Recovery. Then the process server uses this account to install the Mobility service when replication is enabled.
  - This account will only be used by Site Recovery for the push installation, and to update the Mobility service.
  - If you’re not using a domain account, you need to disable Remote User Access control on the VM:
    - In the registry, create DWORD value **LocalAccountTokenFilterPolicy** under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.
    - Set the value to 1.
    - To do this at the command prompt, type the following: `REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1`.
- In the Windows Firewall on the VM you want to replicate, allow File and Printer Sharing, and WMI.
  - To do this, run `wf.msc` to open the Windows Firewall console. Right click **Inbound Rules** > **New Rule**. Select **Predefined**, and choose **File and Printer sharing** from the list. Complete the wizard, select to
allow the connection > **Finish**.

- For domain computers, you can use a GPO to do this.

**Linux machines**

- Ensure that there’s network connectivity between the Linux computer and the process server.
- On the machine for which you enable replication, you need an account that’s a root user on the source Linux server:
  - You specify this account when you set up Site Recovery. Then the process server uses this account to install the Mobility service when replication is enabled.
  - This account will only be used by Site Recovery for the push installation, and to update the Mobility service.
- Check that the /etc/hosts file on the source Linux server has entries that map the local hostname to IP addresses associated with all network adapters.
- Install the latest openssh, openssh-server, and openssl packages on the computer that you want to replicate.
- Ensure that Secure Shell (SSH) is enabled and running on port 22.
- Enable SFTP subsystem and password authentication in the sshd_config file:
  1. To do this, sign in as root.
  2. Find the line that begins with **PasswordAuthentication**, in the /etc/ssh/sshd_config file. Uncomment the line and change the value to **yes**.
  3. Find the line that begins with **Subsystem** and uncomment the line.

    ```
    # override default of no subsystems
    Subsystem    sftp    /usr/libexec/openssh/sftp-server
    ```

  4. Restart the sshd service.

**Note the VM private IP address**

For each machine you want to replicate, find the IP address:

1. In the Azure Stack Portal, click on the VM.
2. On the **Resource** menu, click **Network Interfaces**.
3. Note down the private IP address.

**Step 2: Create a vault and select a replication goal**

1. In the Azure portal, select **Create a resource** > **Management Tools** > **Backup and Site Recovery**.
2. In **Name**, enter a friendly name to identify the vault.
3. In **Resource group**, create or select a resource group. We’re using **contosoRG**.
4. In **Location**, enter the Azure region. We’re using **West Europe**.

5. To quickly access the vault from the dashboard, select **Pin to dashboard > Create**.

![Recovery Services vault](image)

The new vault appears on **Dashboard > All resources**, and on the main **Recovery Services vaults** page.

**Select a replication goal**

1. In **Recovery Services vaults**, specify a vault name. We’re using **ContosoVMVault**.

2. In **Getting Started**, select Site Recovery. Then select **Prepare Infrastructure**.

3. In **Protection goal > Where are your machines located**, select **On-premises**.

4. In **Where do you want to replicate your machines**, select **To Azure**.

5. In **Are your machines virtualized**, select **Not virtualized/Other**. Then select **OK**.
Step 3: Set up the source environment

Set up the configuration server machine, register it in the vault, and discover machines you want to replicate.

1. Click Prepare Infrastructure > Source.

2. In Prepare source, click +Configuration server.

3. In Add Server, check that Configuration Server appears in Server type.

5. Download the vault registration key. You need the registration key when you run Unified Setup. The key is valid for five days after you generate it.

Run Azure Site Recovery Unified Setup

To install and register the configuration server, do an RDP connection to the VM you want to use for the configuration server, and run Unified Setup.

Before you start, make sure that the clock is synchronized with a time server on the VM before you start. Installation fails if the time is more than five minutes off local time.

Now install the configuration server:

1. Run the Unified Setup installation file.

2. In Before You Begin, select Install the configuration server and process server.
3. In **Third Party Software License**, click **I Accept** to download and install MySQL.

4. In **Registration**, select the registration key you downloaded from the vault.
5. In **Internet Settings**, specify how the Provider running on the configuration server connects to Azure Site Recovery over the Internet. Make sure you've allowed the required URLs.

   - If you want to connect with the proxy that's currently set up on the machine, select **Connect to Azure Site Recovery using a proxy server**.
   - If you want the Provider to connect directly, select **Connect directly to Azure Site Recovery without a proxy server**.
   - If the existing proxy requires authentication, or if you want to use a custom proxy for the Provider connection, select **Connect with custom proxy settings**, and specify the address, port, and credentials.

6. In **Prerequisites Check**, Setup runs a check to make sure that installation can run. If a warning appears about the **Global time sync check**, verify that the time on the system clock (**Date and Time** settings) is the same as the time zone.
7. In **MySQL Configuration**, create credentials for logging on to the MySQL server instance that is installed.

8. In **Environment Details**, select No if you’re replicating Azure Stack VMs or physical servers.

9. In **Install Location**, select where you want to install the binaries and store the cache. The drive you select must have at least 5 GB of disk space available, but we recommend a cache drive with at least 600 GB of free space.
10. In **Network Selection**, first select the NIC that the in-built process server uses for discovery and push installation of mobility service on source machines, and then select the NIC that Configuration Server uses for connectivity with Azure. Port 9443 is the default port used for sending and receiving replication traffic, but you can modify this port number to suit your environment's requirements. In addition to the port 9443, we also open port 443, which is used by a web server to orchestrate replication operations. Do not use port 443 for sending or receiving replication traffic.

11. In **Summary**, review the information and click **Install**. When installation finishes, a passphrase is generated. You will need this when you enable replication, so copy it and keep it in a secure location.
After registration finishes, the server is displayed on the Settings > Servers blade in the vault.

NOTE
The configuration server can also be installed from the command line. Learn more.

It can take 15 minutes or more for the account name to appear in the portal. To update immediately, select Configuration Servers > server name > Refresh Server.

Step 4: Set up the target environment

Select and verify target resources.

1. In Prepare infrastructure > Target, select the Azure subscription you want to use.
2. Specify the target deployment model.
3. Site Recovery checks that you have one or more compatible Azure storage accounts and networks. If it doesn’t find them, you need to create at least one storage account and virtual network, in order to complete the wizard.

Step 5: Enable replication

Create a replication policy

1. Click Prepare Infrastructure > Replication Settings.
2. In Create replication policy, specify a policy name.
3. In RPO threshold, specify the recovery point objective (RPO) limit.
   - Recovery points for replicated data are created in accordance with the time set.
   - This setting does not affect replication, which is continuous. It simply issues an alert if the threshold limit is reached without a recovery point being created.
4. In Recovery point retention, specify how long each recovery point is kept. Replicated VMs can be recovered to any point in the specified time window.
5. In App-consistent snapshot frequency, specify how often application-consistent snapshots are created.
An app-consistent snapshot is a point-in-time snapshot of the app data inside the VM.
Volume Shadow Copy Service (VSS) ensures that apps on the VM are in a consistent state when the snapshot is taken.

6. Select **OK** to create the policy.

**Confirm deployment planning**
You can skip this step right now. In **Deployment Planning** dropdown list, click **Yes, I have done it**.

**Enable replication**
Make sure you’ve completed all the tasks in **Step 1: Prepare machine**. Then enable replication as follows:

1. Select **Replicate application** > **Source**.
2. In **Source**, select the configuration server.
3. In **Machine type**, select **Physical machines**.
4. Select the process server (configuration server). Then click **OK**.
5. In **Target**, select the subscription and the resource group in which you want to create the VMs after failover. Choose the deployment model that you want to use for the failed-over VMs.
6. Select the Azure storage account in which you want to store the replicated data.
7. Select the Azure network and subnet to which Azure VMs connect when they’re created after failover.
8. Select **Configure now for selected machines** to apply the network setting to all machines you select for protection. Select **Configure later** if you want to select the Azure network separately for each machine.
9. In **Physical Machines**, click +**Physical machine**. Specify the name, IP address and OS type of each machine you want to replicate.
   - Use the internal IP address of the machine.
   - If you specify the public IP address, replication may not work as expected.
10. In **Properties** > **Configure properties**, select the account that the process server will use to automatically install Mobility Service on the machine.
11. In **Replication settings** > **Configure replication settings**, check that the correct replication policy is selected.
12. Click **Enable Replication**.
13. Track progress of the **Enable Protection** job in **Settings** > **Jobs** > **Site Recovery Jobs**. After the **Finalize Protection** job runs, the machine is ready for failover.

**NOTE**
Site Recovery installs Mobility Service when replication is enabled for a VM.
It can take 15 minutes or longer for changes to take effect and appear in the portal.
To monitor VMs you add, check the last discovered time for VMs in **Configuration Servers** > **Last Contact At**. To add VMs without waiting for the scheduled discovery, highlight the configuration server (don’t select it) and select **Refresh**.

**Step 6: Run a disaster recovery drill**
You run a test failover to Azure to make sure that everything’s working as expected. This failover won’t affect your production environment.
Verify machine properties

Before you run a test failover, verify the machine properties, and make sure that they comply with Azure requirements. You can view and modify properties as follows:

1. In Protected Items, click Replicated Items > VM.

2. In the Replicated item pane, there's a summary of VM information, health status, and the latest available recovery points. Click Properties to view more details.

3. In Compute and Network, modify settings as needed.
   - You can modify the Azure VM name, resource group, target size, availability set, and managed disk settings.
   - You can also view and modify network settings. These include the network/subnet to which the Azure VM is joined after failover, and the IP address that will be assigned to the VM.

4. In Disks, view information about the operating system and data disks on the VM.

Run a test failover

When you run a test failover, the following happens:

1. A prerequisites check runs to make sure all of the conditions required for failover are in place.

2. Failover processes the data using the specified recovery point:
   - Latest processed: The machine fails over to the latest recovery point processed by Site Recovery. The time stamp is shown. With this option, no time is spent processing data, so it provides a low RTO (recovery time objective).
   - Latest app-consistent: The machine fails over to the latest app-consistent recovery point.
   - Custom: Select the recovery point used for failover.

3. An Azure VM is created using the processed data.

4. Test failover can automatically clean up Azure VMs created during the drill.

Run a test failover for a VM as follows:

1. In Settings > Replicated Items, click the VM > +Test Failover.

2. For this walkthrough, we'll select to use the Latest processed recovery point.

3. In Test Failover, select the target Azure network.

4. Click OK to begin the failover.

5. Track progress by clicking on the VM to open its properties. Or, click the Test Failover job in vault name > Settings > Jobs > Site Recovery jobs.

6. After the failover finishes, the replica Azure VM appears in the Azure portal > Virtual Machines. Check that the VM is the appropriate size, connected to the right network, and running.

7. You should now be able to connect to the replicated VM in Azure. Learn more.

8. To delete Azure VMs created during the test failover, click Cleanup test failover on the VM. In Notes, save any observations associated with the test failover.

Fail over and fail back

After you've set up replication, and run a drill to make sure everything's working, you can fail machines over to Azure as required.

Before you run a failover, if you want to connect to the machine in Azure after the failover, then prepare to connect before you start.

Then run a failover as follows:
1. In Settings > Replicated Items, click the machine > Failover.
2. Select the recovery point that you want to use.
3. In Test Failover, select the target Azure network.
4. Select Shut down machine before beginning failover. With this setting, Site Recovery tries to shut down the source machine before starting the failover. However failover continues even if shutdown fails.
5. Click OK to begin the failover. You can follow the failover progress on the Jobs page.
6. After the failover finishes, the replica Azure VM appears in the Azure portal > Virtual Machines. If you prepared to connect after failover, check that the VM is the appropriate size, connected to the right network, and running.
7. After verifying the VM, click Commit to finish the failover. This deletes all available recovery points.

**WARNING**
Don't cancel a failover in progress: Before failover is started, VM replication is stopped. If you cancel a failover in progress, failover stops, but the VM won't replicate again.

**Fail back to Azure Stack**
When your primary site is up and running again, you can fail back from Azure to Azure Stack. To do this, you need to download the Azure VM VHD, and upload it to Azure Stack.

1. Shut down the Azure VM, so that the VHD can be downloaded.
2. To start downloading the VHD, install Azure Storage Explorer.
3. Navigate to the VM in the Azure Portal (using the VM name).
4. In Disks, click on the disk name, and gather settings.
   - As an example, the VHD URI used in our test:
     https://502055westcentralus.blob.core.windows.net/wahv9b8d2ceb284fb59287/copied-3676553984.vhd can be broken down to get the following input parameters that are used to download the VHD.
     - Storage Account: 502055westcentralus
     - Container: wahv9b8d2ceb284fb59287
     - VHD Name: copied-3676553984.vhd
5. Now, use Azure Storage Explorer to download the VHD.
6. Upload the VHD to Azure Stack with these steps.
7. In the existing VM or new VM, attach the uploaded VHDs.
8. Check that the OS Disk is correct, and start the VM.

At this stage failback is complete.

**Conclusion**
In this article we replicated Azure Stack VMs to Azure. With replication in place, we ran a disaster recovery drill to make sure failover to Azure worked as expected. The article also included steps for running a full failover to Azure, and failing back to Azure Stack.

**Next steps**
After failing back, you can reprotect the VM and start replicating it to Azure again. To do this, repeat the steps in this article.